ElectioNet™

State of New Jersey Office of the Attorney General Division of Elections

Documentation of the Network Infrastructure for the Statewide Voter Registration System (SVRS)

NEW JERSEY

Deliverable SVRS 011

Presented to:
Michael Gallagher
SVRS Project Manager
Department of Law and Public Safety
Trenton, New Jersey

Presented by:
Covansys Corporation
32605 West 12 Mile Road
Farmington Hills, MI 48334

July 2005

Revision History

Date	Brief Description	Changed By:
05/02/2005	Initial Draft	Wm. Gary Bush
05/02/2005	ATS Update	Chad Duling
05/12/2005	PCC Update	Raj Satyaneni
05/18/2005	Final Formatting and Review	Wm. Gary Bush
06/22/2005	ATS Update	Elissa Smith
07/21/2005	Formatting and Content Review/Update – Version 1	Chris Kluesener

Table of Contents

Overview ______________________________ **1**

Networking Details ______________________________ **2**

OVERVIEW

For the SVRS project, Covansys has partnered with AT&T as its primary provider of network services. As the network service provider, AT&T is responsible for the networking connections to both hosting sites and all counties.

Throughout the project, AT&T will be setting up a Multi-protocol Label Switching (MPLS) network for the State of New Jersey which offers a private network between each county and the host environments. This MPLS Network will only include the inter-connectivity between counties and the host environments lacking Internet connectivity. AT&T's network strategy includes a MPLS core that adds efficient label forwarding to our IP Networks.

AT&T's network maintains a high level of reliability with redundant, diverse paths to avoid single points of failure and provide optimal routing and traffic flow, as well as uninterruptible power supply at every switching node.

This deliverable is an adjunct to SVRS039, also titled "Documentation of the Network Infrastructure". This document, SVRS011, focuses on the AT&T MPLS network and the firewall devices used to secure that access.

NETWORKING DETAILS

The MPLS network is responsible for routing each county's 10.160.X.X IP addresses with the host environment. Each IP packet will be forwarded after the IP header is examined once and then a MPLS label is assigned. This label is another way to authenticate a county's IP address is a part of the MPLS network. All forwarding will use that same label, avoiding the need for an IP header lookup at each hop. The network is also protected against MPLS spoofing, so that packets with unauthorized labels cannot be injected into the network. AT&T is responsible for managing the MPLS Network.

In conjunction with the MPLS network, Covansys will setup the SonicWall firewall in all the counties, and PIX firewall at the host environment. Both types of firewalls are described below.

PIX Firewall Setup at Production Site.

The Cisco PIX 515E firewall is the purpose-built security appliance that delivers enterprise-class security for small to medium-sized business networks. The PIX 515E is the one-rack-unit design that supports up to six 10/100 Fast Ethernet interfaces, making it an excellent choice for businesses requiring a cost-effective, resilient security solution with "demilitarized zone" support. The PIX provides full, automatic failover by using a failover cable and stateful failover using a crossover cable.

The PIX Firewall contains six 10/100 Ethernet interfaces (Inside, Outside, 4 port FE Card).

Inside Port – AT&T MPLS Network

Outside Port – Internet Segment Network

Interface 2 – Environment Server Segment (10.160.45.x)

Interface 3 – DMZ Segment

Interface 5 - Stateful Failover (connection to failover box with crossover cable)

State and county SVRS users with connectivity to the MPLS network will access the system through the Inside Interface (AT&T MPLS Cloud), whereas all other traffic will be routed through Outside Interface. Covansys will only open the required ports across the firewall so that servers will be more secure.

Sonic Wall Firewall Setup at County Site

The SonicWall is the ultimate total security platform for small and remote office deployments. The SonicWall allows rapid deployment in basic networks with a user-friendly Web interface and powerful wizards. This high performance deep packet inspection firewall includes SonicOS, allowing multiple node configurations and offers a choice between absolute ease of use for basic networks and ultimate flexibility for networks with more complex needs.

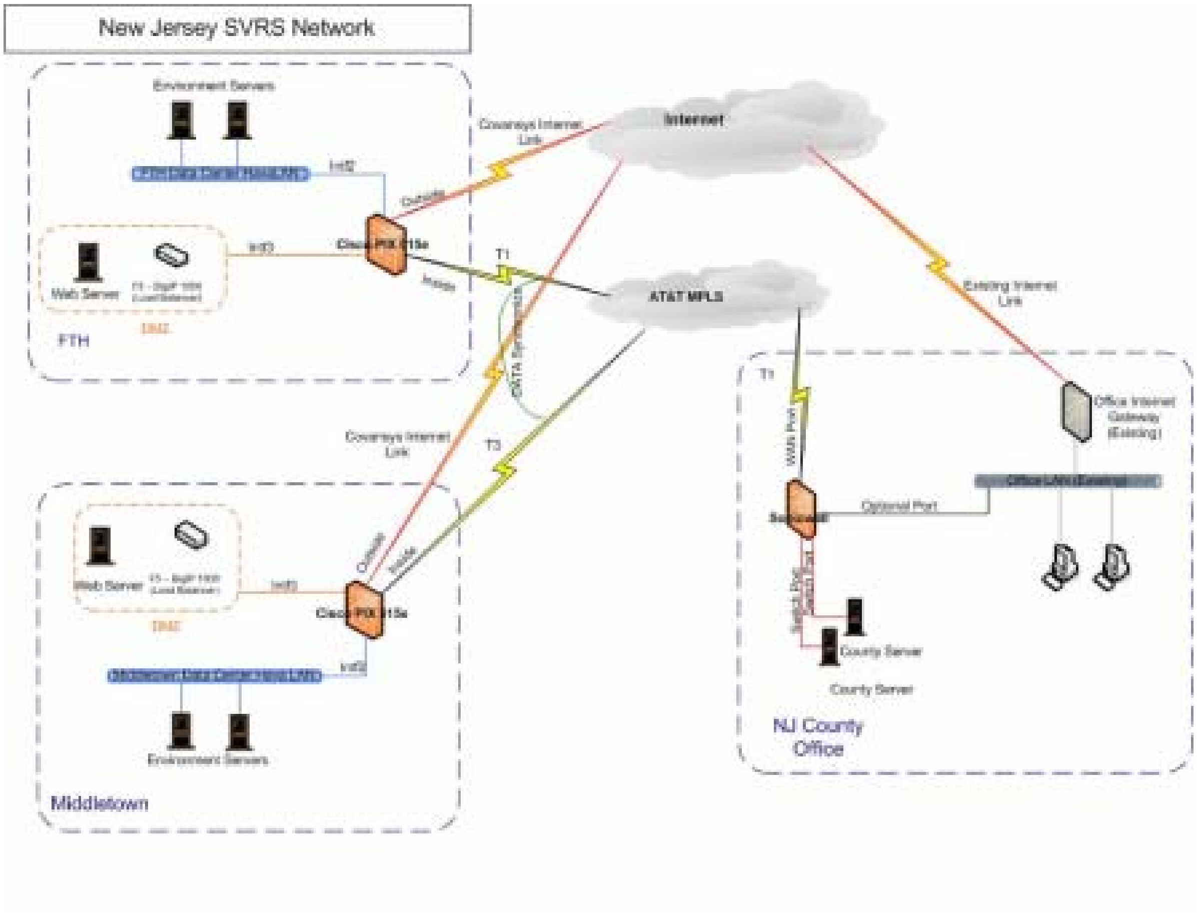
The SonicWall consists of seven 10/100 Ethernet Interfaces (1 WAN, 1 Optional, 1 5-Port LAN Switch)

WAN Port - AT&T MPLS Network

LAN Switch Port – County HAVA Server Segment (10.160.X.X)

Optional Port – Connect to the Existing County LAN (if applicable)

State and county SVRS users will access the system through web browsers on their desktop workstations.   Once connected to the URL (10.160.X.X), the traffic will flow through the SonicWall firewall (Optional Port to LAN Switch Port) before gaining access to the county servers. Covansys will open only the required ports across the firewall so that the servers will be more secure.



Further explanation of the network infrastructure can be found in SVRS039